TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Workforce Security

HIPAA Security • November 2003

Standard Requirement

As part of their administrative safeguards, covered entities are required to implement a workforce security program. Workforce Security is defined as the implementation of policies and procedures to ensure that all members of the workforce have appropriate access to electronic protected health information (EPHI). The term "workforce" includes all personnel, even those that are not directly involved in patient care, like cleaning personnel or the occasional maintenance or repair contractor. Other examples include full-time employees and part-time employees, contract personnel, volunteers, students and trainees.

Workforce Security has three implementation specifications, all of which are addressable:

- Authorization and/or supervision
- Workforce clearance procedure
- Termination procedures

Implementation Specifications

The first specification includes implementing procedures for the authorization and/or supervision of workforce members who work directly with EPHI or who work in locations where they could access the information. This means that an employee who works in an area where EPHI is stored, would either have authorization to the information or require supervision by someone who does. Because this specification is addressable, compliance by the covered entity depends on the results of their risk assessment. If their risk assessment determines that threats exist from members of the workforce working with or in locations accessible to EPHI, the covered entity is required to implement procedures to ensure workforce members working in those locations are either authorized to be there, supervised while there or both. The choice may vary across different types of workers depending on the results of the risk analysis, cost and a covered entity's resources and business processes. The text broadens the criteria to include those with physical access to the network that do not necessarily have authorization or a "need-to-know" for information on the network. The risk management plan should document the results and justify all actions taken in response to the risk assessment.

The second specification, workforce clearance procedure, determines the appropriateness of a workforce member's access to EPHI. Like the previous specification, this requirement is addressable. A covered entity's compliance depends on the outcome of their risk assessment, which determines whether or not the access to the EPHI is

Workforce Security

appropriate. The word "clearance" does not mean a government or military style clearance, but rather a process for determining a person's trustworthiness. "Clearance" does mean that a workforce member's access to EPHI will depend on assessments of their job responsibilities including the amount and type of supervision. This means that an organization should implement a screening process to use for each job position or role and document the procedures to be followed in conducting that check. While some roles may require job references or a National Agency Check (NAC), others may not require any process beyond an interview.

The third specification, termination procedures, focuses on two common threats. The first threat is continued access to information by terminated employees. Employment can end for many different reasons such as retirement, change of jobs, or unsatisfactory performance with each reason potentially posing different threats to information assets. Depending upon its risk assessment, an organization may require different procedures for terminating a former employee's access to information. Some procedures may include deactivating userids and passwords, turning in keys, tokens or cards, or removing the employee from access lists. The appropriateness of the procedures is determined by the size and type of the organization. The second threat is continued access to information by those who are still employees but whose access is no longer appropriate. A covered entity should implement and document procedures for terminating access when required by the clearance process.

See also:
45 CFR 164.308(a)(3)

Federal and DoD regulations that support this standard
DoDD 5200.2
DoDR 5200.2
DoD 8510.1-M
DoDD 8500.1
DoDI 8500.2